Fehlerkorrektur

Notwendigkeit und Probleme der Quanten-Fehlerkorrektur

- Qbits müssen komplett isoliert von der Rechnerumgebung sein.
- Unmöglich, d.h. die Umgebung degeneriert Quantenzustände.
- Beobachtung von Fehlern durch Messung zerstört Zustand.
- Amplituden sind nicht diskret.
- D.h. Bitflips sind nicht die einzigen möglichen Fehler.
- Z.B. können einfache Phasenflips $|0\rangle + |1\rangle \mapsto |0\rangle - |1\rangle$ auftreten.
- Diese Fehler sind durch Messung nicht zu erkennen.

Klassisch:

- Auftretende Fehler sind ausschließlich Bitflips.
- Einfachste Lösung ist ein Repetitionscode der Länge 3.
- Wir codieren $0 \mapsto 000$ und $1 \mapsto 111$.
- Code erkennt zwei Fehler und korrigiert einen Fehler.

Repetition für Quanten

3-Qubit Repetition

Gegeben: Zustand $|z\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
Gesucht: Zustand $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$

Lösung:

- Verwende zwei Hilfsbits in Zustand $|0\rangle$, d.h. $|z00\rangle$.
- Kopiere die Basiszustände mittels CNOT.
- Sei C_{ij} ein CNOT auf Qubit j mit Kontrollbit i. Es gilt
$$|r\rangle = C_{12}C_{13}(\alpha_0|000\rangle + \alpha_1|100\rangle) = \alpha_0|000\rangle + \alpha_1|111\rangle.$$

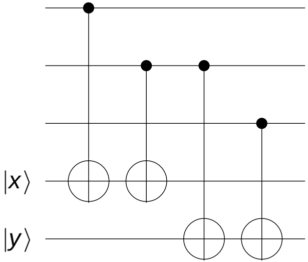
Fehlermodell:

- Wir nehmen vereinfachend an, dass nur Bitflips auftreten.
- D.h. unsere fehlerbehafteten Zustände sind
$$\begin{aligned} |e_1\rangle &= \alpha_0|100\rangle + \alpha_1|011\rangle \\ |e_2\rangle &= \alpha_0|010\rangle + \alpha_1|101\rangle \\ |e_3\rangle &= \alpha_0|001\rangle + \alpha_1|110\rangle. \end{aligned}$$
- Wir müssen Fehler beobachten, ohne zu messen.

Beobachten von Fehlern

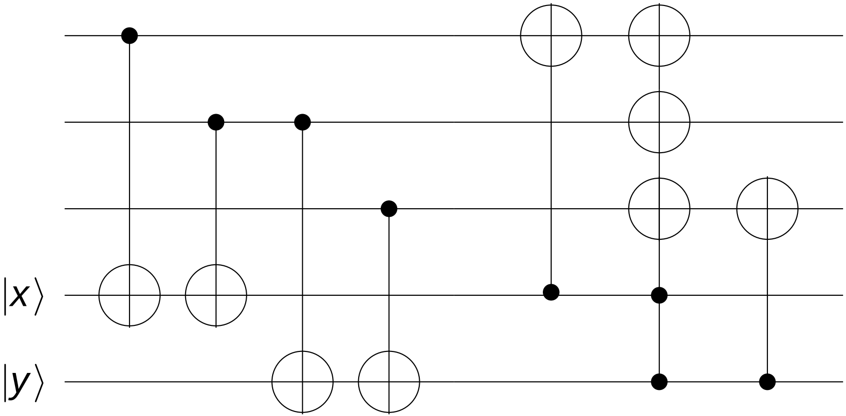
Beobachtung von Bitflips

- Wir verwenden zwei weitere Hilfsbits $|xy\rangle$, initialisiert mit $|0\rangle$.
- Das folgende Gatter erhält als Eingabe $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$.
- Auftretende Bitflips werden mit CNOT-Gattern wie folgt kopiert.



- **Fall 1** fehlerfrei: $|xy\rangle = |00\rangle$.
- **Fall 2** Bitflip $|e_1\rangle$: $|xy\rangle = |10\rangle$.
- **Fall 3** Bitflip $|e_2\rangle$: $|xy\rangle = |11\rangle$.
- **Fall 4** Bitflip $|e_3\rangle$: $|xy\rangle = |01\rangle$.
- D.h. durch *Messung der Hilfsbits* $|xy\rangle$ erkennen wir einen Fehler.
- Wir nutzen nur Relationen zwischen den ursprünglichen Bits.
- Der ursprüngliche Zustand bleibt in seiner Superposition erhalten.

Korrektur der Fehler



Korrigieren allgemeiner Fehler

Fakt 5-Qubit Code

Es existiert ein 5-Qubit Code zum Korrigieren eines generellen 1-Qubit Fehlers.

- Code korrigiert nicht nur Bit-Flips, sondern auch Phasenfehler.

Bit Commitments

Bit Commitment informal

1. **Commitment-Phase:**
   - Alice platziert ein Bit $b \in \{0, 1\}$ in einem Safe.
   - Alice sendet den Safe an Bob.
   - Bob kann den Safe nicht einsehen, lernt also nichts über b.
     (Concealing Eigenschaft)
2. **Revealing-Phase:**
   - Alice öffnet den Safe und zeigt Bob das Bit b.
   - Alice kann ihr Bit dabei nicht ändern.
     (Binding Eigenschaft)

Realisierung mittels Qubits

Protokoll Quanten Bit Commitment

Sicherheitsparameter: n

Commitment-Phase:

- Alice wählt $\mathbf{x} \in_R \{0,1\}^n$.
- **Fall 1** $b = 0$: Alice sendet $|\mathbf{y}\rangle = |\mathbf{x}\rangle$ an Bob.
- **Fall 2** $b = 1$: Alice sendet $|\mathbf{y}\rangle = H_n|\mathbf{x}\rangle$ an Bob.

Revealing-Phase:

- Alice sendet b und $\mathbf{x}$ an Bob.
- Bob misst $H_n^b|\mathbf{y}\rangle$ in der Standardbasis und vergleicht mit $|\mathbf{x}\rangle$.

Anmerkungen:

- **Conceiling:** Falls Bob in der Standard- oder der Hadamardbasis misst, erhält er 0 bzw. 1 jeweils mit Ws $\frac{1}{2}$.
- **Binding:** Falls $b' \neq b$, gilt $\mathbf{x} = \mathbf{y}$ nur mit Ws 2^{-n}.

Betrügerische Alice

Protokoll Betrügerische Alice

Sicherheitsparameter n

Commitment-Phase:

- Alice wählt n EPR-Paare $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice sendet jeweils das zweite Bit an Bob.

Revealing-Phase:

- **Fall 1:** $b = 0$: Alice misst ihr erstes Bit aller n Paare $|e\rangle$.
- **Fall 2:** $b = 1$: Alice berechnet $H|e\rangle$ und misst ihre n Qubits.
- Sei $\mathbf{x}$ das Ergebnis der Messung. Sende $b, |\mathbf{x}\rangle$ an Bob.

Anmerkung:

- Für $b = 0$ misst Bob aufgrund der Verschränkung dasselbe.
- Für $b = 1$ gilt $(H \otimes H)|e\rangle = |e\rangle$.
- D.h. auch in diesem Fall messen Alice und Bob dasselbe.

Sicheres Quanten Bit Commitment

Offenes Problem Quanten Bit Commitment

Existiert ein sicheres Quanten Bit Commitment Protokoll?

Anmerkung:

- Mayers 1996: Generische Attacke gegen Quanten BC Protokolle.
- Vermutung: Sichere Quanten-BC Protokolle sind nicht ohne weitere Annahmen konstruierbar.